



Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 20 September 2004

Current Nationwide
Threat Level is



[For info click here](http://www.whitehouse.gov/homeland)
www.whitehouse.gov/homeland

Daily Overview

- The Transportation Security Administration has announced new passenger screening procedures that will increase the use of explosives trace detectors, expand the use of manual pat-down searches, and give screeners more latitude to refer individuals to secondary screening. (See item [10](#))
- The Tampa Bay Business Journal reports University of South Florida microbiologists say they have developed tests that can rapidly identify anthrax and smallpox, in the event of a suspected bioterror attack. (See item [18](#))
- The US-CERT has released “Technical Cyber Security Alert TA04-261A: Multiple vulnerabilities in Mozilla products.” (See item [22](#))

DHS/IAIP Update Fast Jump

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS/IAIP Web Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. *September 16, Reuters* — **Hurricane Ivan uproots oil rigs.** Hurricane Ivan, which devastated the Caribbean, wrought havoc on oil drilling operations in the Gulf of Mexico. **One deepwater semi-submersible rig was torn from its moorings and later found 70 miles away, while an oil drilling rig took a direct hit from Ivan and was set adrift and sustained damage, the off-shore companies said.** Dallas, TX-based ENSCO International Inc. said one of its jack-up drilling rigs, ENSCO 64, was directly in the path of the hurricane. ENSCO said the rig

sustained damage and was afloat in the Gulf approximately 80 miles southeast of Venice, LA. The off-shore oil drilling contractor Transocean Inc. said its semi-submersible rig Deepwater Nautilus went missing after the hurricane roared across the Gulf. It was later found 70 miles away.

Source: <http://www.nytimes.com/reuters/business/business-weather-ivan-rigs.html>

[\[Return to top\]](#)

Chemical Industry and Hazardous Materials Sector

2. *September 19, Agence France Presse* — **More toxic materials set to join global trade watch list.** Up to 15 hazardous substances are expected to be added to a "watch list" regulating international trade in toxic industrial products and pesticides, the UN's environmental agency said. **The inclusion of the substances, including tetraethyl lead, an additive used in some petrol, and several types of asbestos, will be up for discussion at a high-level international conference in Geneva starting Monday, September 20.** The five-day conference on the Rotterdam Convention, which entered into force in February 2004, is expected to bring together ministers and officials from the 74 countries involved in the treaty, as well as 50 more as observers. "The Rotterdam Convention provides the first line of defense for human health and the environment against the potential dangers of hazardous chemicals and pesticides," said Klaus Toepfer, executive director of the UN Environment Program (UNEP). Under the treaty, any exports of the 22 pesticides and five chemicals currently on the list must be approved by the importing country. It also imposes an international alert system for transfers of the hazardous materials. The inclusion of one of the 15 candidate substances, chrysotile asbestos, used mainly for construction materials in developing countries, is likely to face opposition from two of its biggest producers, Canada and Russia, officials said.

Source: http://www.channelnewsasia.com/stories/afp_world/view/107392/1/.html

[\[Return to top\]](#)

Defense Industrial Base Sector

3. *September 18, MSNBC* — **Florida Navy base sustains extensive damage.** Hurricane Ivan inflicted "catastrophic" damage on the Pensacola Naval Air Station in Florida and the base may not reopen for two weeks, Navy officials said on Friday, September 17. **A spokesperson for the Navy said that Ivan caused "hundreds of millions of dollars" in damage at the 82-acre National Historic Landmark, damaging every building and destroying several edifices on the grounds.** At the base hospital, the storm left several holes in the roof and caused an estimated \$200,000 to \$500,000 in damage. The 19 patients were not injured, having been moved by medical personnel to a safe location inside the building. At least 480 sailors were evacuated and most of the base's aircraft were flown inland before the storm to avoid potential damage before Ivan stormed ashore. There were no reports of injuries among the personnel who stayed at the base during the storm, the officials said. Pensacola is the Navy's traditional home of naval aviation and thousands of pilots receive training there each year.

Source: <http://msnbc.msn.com/id/6028506/>

4. *September 16, American Forces Press Service* — **War on terror testing, reinforcing Air Force concepts. The war on terror is teaching the Air Force important lessons and validating others, according to Air Force Secretary James G. Roche. It is emphasizing the success of the Air Expeditionary Force, the importance of joint operations, and the critical contribution of the Guard and Reserve in the total force, he said.** Operations in Iraq and Afghanistan underscore the value of the Air Expeditionary Force. A highly specialized force Roche said, it can respond in an instant's notice and is able to go great distances. Roche said frequent operational deployments keep the Air Expeditionary Force trained for whatever missions come their way. When the Air Force flew into Afghanistan during the first night of Operation Enduring Freedom, for example, 70 to 75 percent of the Air Force pilots involved had already been combat tested — thanks to 12 years of patrolling northern and southern Iraqi skies during operations Northern Watch and Southern Watch. Roche said the war on terror has caused the services to focus closely on who was doing what and who could do it most efficiently, so in addition to providing precise, close-air support for ground troops, the Air Force works provides direct support to Navy SEALs and Army Special Forces troops.
Source: http://www.defenselink.mil/news/Sep2004/n09162004_2004091612.html

[[Return to top](#)]

Banking and Finance Sector

5. *September 17, The Irish Independent* — **E-mail scam targets bank clients.** Banks believe a gang with links to the Russian mafia is behind an e-mail scam which on Thursday, September 16, tried to obtain account details from hundreds of AIB Bank customers in Ireland. It is the second time fraudsters have struck in Ireland by sending e-mails bearing bank logos and requesting information by claiming it was part of a software upgrade by the banks' technical services departments. **Ireland has been targeted as part of a worldwide scam, in which an estimated two billion e-mails purporting to come from banks are sent out annually, achieving a 19 percent success rate.** Una Dillon, manger of the Irish Payment Services Organization card services and a member of a European Union fraud expert group, said experience elsewhere in Europe suggested gangs possibly linked to the Russian mafia were behind the scams.
Source: <http://home.eircom.net/content/unison/national/4025676?view=Eircomnet>
6. *September 17, Northern Territory News (Australia)* — **Credit card details stolen.** Thousands of dollars are being stolen from the credit cards of residents of the Northern Territory in Australia who are vacationing in South-East Asia. **A major Australian bank confirmed international credit card fraud had risen recently, particularly in Malaysia. The numbers are being stolen via a skimming scheme, where the credit card is swiped through a machine that copies the details on the magnetic strip.** A counterfeit card is then made and the thief goes on a shopping spree, usually targeting expensive items such as jewelry and electronics — all charged to the card owner's account. ANZ bank spokesperson Paul Edwards said a bank computer tracked customer card use for suspicious transactions. Edwards said the bank also cancelled cards if customers had visited parts of South-East Asia considered high risk. “We do take a few more precautions with cardholders who visited Malaysia — if they have visited a particular area or region that is prone to fraud or skimming we will act,” he said.
Source: http://www.news.com.au/common/story_page/0,4057,10791246%255E13569,00.html

7. *September 17, New York Times* — **Men indicted in fund-raising for terrorists. Two men were charged in a federal indictment on Thursday, September 16, with raising money to support terrorists and recruiting would-be terrorists to fight in Afghanistan, Chechnya, Kosovo and Somalia.** The indictment, by a grand jury in Miami, FL, said the men had discussed recruiting an unidentified American paid to train in the Mideast. The two men indicted were already facing criminal charges here and in Egypt. Attorney General John Ashcroft identified them as Adham Amin Hassoun, who also goes by the name Abu Sayyaf, and Mohamed Hesham Youssef, who also goes by the name Abu Turab. Both are charged with conspiracy to provide material support to terrorists. **The indictment charges that Hassoun wrote checks from 1994 to late 2001 to unindicted co-conspirators and groups, including the Holy Land Foundation and the Global Relief Foundation, to support jihad.** The two groups reportedly have ties to terrorism financing. The 10-count indictment also charges that the men had coded conversations from 1996 through 2000 that suggested participation in jihad in Afghanistan, Chechnya, Kosovo and Somalia.

Source: <http://www.nytimes.com/2004/09/17/politics/17terror.html>

[[Return to top](#)]

Transportation Sector

8. *September 18, Associated Press* — **Plane makes emergency landing in Chicago. An American Airlines jetliner made an emergency landing Thursday, September 16, at O'Hare International Airport in Chicago, after its left engine caught fire, apparently when a goose was sucked into the engine shortly after takeoff.** The plane, an MD-80 carrying 112 people, landed safely and there were no injuries. As the Philadelphia-bound plane rose into the air, several people on the ground said they heard an explosion overhead and saw flames shooting from the engine, Chicago Fire Department officials said. In neighborhoods around O'Hare, authorities found pieces of metal debris believed to have fallen from the airplane. No injuries or damage were immediately reported on the ground.
Source: http://story.news.yahoo.com/news?tmpl=story&cid=519&ncid=718&e=10&u=/ap/20040917/ap_on_re_us/american_emergency_landing
9. *September 18, Oakland Tribune* — **Security breach empties Oakland airport.** Security teams double-checked bag screening machines and cameras, plus interviewing passenger screeners at Oakland International Airport to find out how and why somebody got through with contraband on Thursday, September 16. The breach led to a full evacuation and two hours of waiting as teams with bomb-sniffing dogs scoured the airport and emptied airplanes. **At around 9 p.m., according to airport spokesperson Cyndy Johnson, a "prohibited item" raised warning flags at the screening station in Terminal One. The passenger had slipped into the secure boarding area past a veteran screener who has had no record of disciplinary problems, officials said.** By 9:20 p.m., Oakland police and Transportation Security Administration teams fanned out through both terminals looking for a specific passenger and bag, but found nothing. At that point, Federal Security Director Fred Lau decided to evacuate the terminal and conduct a more thorough sweep. Nothing was found and by 10:10 p.m., the waiting passengers had all been re-screened. By 11 p.m. the first planes departed. **The evacuation interrupted six departing flights, delaying 600 passengers.**

Source: <http://www.oaklandtribune.com/Stories/0.1413.82~1726~2410807.00.html>

10. *September 16, Transportation Security Administration* — **TSA increases level of explosives searches at U.S. airports.** The Transportation Security Administration (TSA) on Thursday, September 16, announced new passenger screening procedures that will increase the use of explosives trace detectors, expand the use of manual pat-down searches, and give screeners more latitude to refer individuals to secondary screening. **The enhancements are designed to strengthen checkpoint screening of passengers and carry-on baggage and are in line with a recent recommendation of the 9/11 Commission Report that all passengers selected for secondary screening be checked for explosives.** Passengers must continue to go through metal detectors and put their carry-on items through the X-ray; the extra measures will be applied to those persons referred to secondary screening. **Beginning next week, the new protocol will also require all passengers to remove outer coats and jackets for X-ray before proceeding through the metal detectors. Included are suit and sport coats, athletic warm-up jackets and blazers. The new measures authorize pat-down searches of passengers if warranted, based on visual observations.** These limited searches will be conducted as part of the secondary screening process.

Source: http://www.tsa.gov/public/display?theme=44&content=090005198_00cdb11

[\[Return to top\]](#)

Postal and Shipping Sector

Nothing to report.

[\[Return to top\]](#)

Agriculture Sector

11. *September 16, Casper Star Tribune (WY)* — **Researcher wants out-of-state deer. Elizabeth Williams with the University of Wyoming College of Agriculture's veterinary sciences wants to bring in 10 mule deer fawns and 10 white-tailed deer fawns for a collaborative epidemiology of chronic wasting disease (CWD. She said the deer will be used as controls for the study, which is being funded by the Department of Defense.** Williams, Terry Kreeger with the Game and Fish Department, and the Colorado Division of Wildlife are conducting the research. The deer would be acquired from Washington, Colorado, Idaho, Kansas, South Dakota, or Nebraska. The animals would be taken from areas not known to have CWD. CWD was first detected in the Rocky Mountain region in 1967, when biologists diagnosed a sick deer at a wildlife research facility in Fort Collins, CO. It was found in Wyoming by the end of the decade at the Game and Fish Department's Sybille Canyon Research Facility and has since been documented in wild herds of both deer and elk. CWD attacks the central nervous system of deer and elk and is 100 percent fatal to animals that contract it.

Source: <http://www.casperstartribune.net/articles/2004/09/16/news/wyoming/4aba398079ab055887256f120001e65b.txt>

12.

September 16, Weekly (GA) — **Fungus threatens trees. Sudden Oak Death (SOD) disease, caused by a fungus introduced into California in the early 1990s, now poses a statewide threat to Georgia's oak trees due to infected plants imported to nurseries.** James Johnson, Forest Health Coordinator for the Georgia Forestry Commission (GFC), said the fungus — *Phytophthora ramorum* — has existed in Europe for many years, but was only identified in the U.S. when SOD began killing oaks in California about five years ago. The fungus affects many of the most popular plants sold in nurseries including camellia, rhododendron, azalea, pieris, viburnum, and lilac. Georgia nurseries in the following counties tested positive for SOD fungus: Coffers Home & Garden Inc., Clarke County; Craven Pottery Inc., Banks County; Deep Springs Nurseries, Whitfield County; Green Thumb West Nursery & Garden, Columbia County; Greenbrier Nursery & Gifts LLC, Columbia County; Island Ace Garden Center, Glynn County; John Deere Landscapes #173, Fulton County; John Deere Landscapes #172, Forsyth County; John Deere Landscapes #57, Gwinnett County; Pike Nursery # 2, Cobb County; Sago Inc. d/b/a Plant Plus, Coffee County; Southeastern Wholesale Nursery # 1, Gwinnett County; Still Lake Nursery Inc., Gwinnett County; and Shemin Nurseries, Gwinnett County. Each has been recently checked by officials and declared "disease free."
Source: http://www.theweekly.com/news/2004/September/16/oak_trees.ht ml

[[Return to top](#)]

Food Sector

Nothing to report.

[[Return to top](#)]

Water Sector

13. *September 17, Lowell Sun (MA)* — **Bleach eyed as source of contamination. Disinfectant used to treat wastewater is being eyed as a possible source of perchlorate contamination in the Merrimack and Concord rivers in Massachusetts after tests found high levels of perchlorate in processed water from the Billerica wastewater treatment plant. Tests have also found perchlorate in water from the Lowell wastewater treatment plant.** The chlorination process could be adding perchlorate to the water, but it is not a certainty, said Ed Kunce, deputy commissioner of the Massachusetts Department of Environmental Protection. If a disinfectant is determined to be a source, it is not necessarily creating the perchlorate recently found in Tewksbury, MA's drinking water, he said. And there is no clear short-term fix. Perchlorate, a compound found in rocket fuel and explosives, is related to chlorine, containing one chlorine molecule. Ingestion of perchlorate is believed to impact the function of the thyroid gland. Tests to find a source have been ongoing since mid-August when Tewksbury found perchlorate at levels above one part per billion in its drinking water and issued a public health advisory. The source of Tewksbury's water is the Merrimack River. Perchlorate has also been detected in water samples from the Concord River in Lowell.
Source: <http://www.lowellsun.com/Stories/0.1413.105~4761~2408759.00. html>

[[Return to top](#)]

Public Health Sector

14. *September 17, Voice of America* — **Soil-based infection.** Singapore says at least 23 people have been killed this year from a soil-based bacterial infection. **Singapore health officials say melioidosis has a mortality rate three times greater than Severe Acute Respiratory Syndrome (SARS).** Melioidosis, also known as Whitmore's Disease, enters the body when bruised skin comes into contact with contaminated soil or water. The illness causes blood poisoning, fever and possible pneumonia and death. There is no vaccine for melioidosis, but the illness can be treated with antibiotics, if detected early. **The U.S. has classified the infection as a potential biological weapon, but Singapore says there is no evidence, it has been spread intentionally.**

Source: <http://www.voanews.com/article.cfm?objectID=7AECD5A8-75B0-447A-8193446388F32F0F&title=Singapore%3A%2023%20Deaths%20from%20Soil-Based%20Bacterial%20Infection&catOID=45C9C78B-88AD-11D4-A57200A0CC5EE46C&categoryname=Asia%20Pacific>

15. *September 17, Associated Press* — **Biodefense research.** Oregon researchers have started work on a new five-year, \$10.3 million biodefense contract to find the proteins associated with bacteria that cause salmonella poisoning and typhoid fever, and the virus that causes monkeypox. The lab at Oregon State University's Vaccine and Gene Therapy Institute is one of the few in the United States with the authorization to conduct research on the monkeypox virus, which is similar to the smallpox virus. Monkeypox was reported for the first time in the U.S. in June 2003 when a Wisconsin girl became ill after her mother bought an infected prairie dog at a swap meet. The disease previously had been seen only in the African rain forest. The project will be coordinated with the Pacific Northwest National Laboratory, which does research for the U.S. Department Of Energy on complex problems in energy, national security, the environment and biology.

Source: http://story.news.yahoo.com/news?tmpl=story&cid=624&ncid=753&e=10&u=ap/20040917/ap_on_sc/biodefense_ohsu

16. *September 17, Post-Standard (NY)* — **Whooping cough outbreak spreads.** By the time the coughing fits begin, a person with pertussis has been spreading germs for a week or two, feeling as if they are tired from a cold rather than threatened by a potential killer. That's why containing the spread of the disease known popularly as whooping cough is so tricky. **Since the outbreak started last fall, in central New York, 160 cases of pertussis have been reported in Onondaga County.** The county usually has 10 cases a year. Ten children have been hospitalized with pertussis since that time. **Health officials in adjacent counties are also concerned about the growing threat of pertussis, which is making a comeback nationwide.** The Centers for Disease Control and Prevention report most cases are among infants and adolescents from ages 10 to 19. The disease has never disappeared since it was identified in the 16th century. Pertussis is an extremely contagious respiratory disease. It causes spasms of coughing that usually end with a high-pitched whooping sound. The bacteria responsible for pertussis is spread through the air by droplets expelled in coughs and sneezes.

Source: <http://www.syracuse.com/news/poststandard/index.ssf?/base/news-1/1095412836114170.xml>

17.

September 17, Lamar Daily News (CO) — **Exercise to provide experience for emergency personnel.** Prowers, CO, will be one site of a mass vaccination clinic exercise which is designed to give local public health and emergency response personnel valuable experience which would help in dealing with a possible bioterrorism attack. The mass vaccination exercise in Prowers County will be conducted on Saturday, October 16. **Similar mass vaccination exercises will also be conducted in other southeastern Colorado counties, including Baca, Bent, Cheyenne, Kiowa, Otero, Crowley, Las Animas, and Huerfano counties.** The event, at which key personnel will be vaccinated to ensure they can proceed with the duties that would be required of them in a real emergency, will give public health and emergency response personnel experience in conducting mass immunizations as would be required in the event of an actual emergency, such as a bioterrorism event or a pandemic influenza outbreak. Key personnel to be vaccinated for flu at the practice event will include first responders, emergency medical technicians, public works personnel, hospital personnel, clinic volunteers, and law enforcement officers and their families. After key personnel have been immunized, members of the public will be able to receive a free flu shot.

Source: <http://www.lamardaily.com/Stories/0,1413,121~7979~2408871,00.html>

18. *September 16, Tampa Bay Business Journal (FL)* — **Smallpox test.** University of South Florida (USF) microbiologists said they have developed tests that can rapidly identify anthrax and smallpox. Used in the field in the event of a suspected bioterror attack, positive rapid testing could prevent disease spread while negative results could prevent panic over fears that an anthrax or smallpox attack has occurred. **Using throat swab samples seeded with Vaccinia virus, a surrogate of smallpox, and a fiber-optic biosensor, the researchers said they could detect the virus in 20 minutes. It also found it could detect moderate concentrations of anthrax in less than an hour directly from powder samples with no false positives with the same biosensor.** Studies reporting the USF findings were recently published in the Journal of Microbiological Methods and in Biosensors & Bioelectronics.

Source: <http://tampabay.bizjournals.com/tampabay/stories/2004/09/13/daily35.html>

[\[Return to top\]](#)

Government Sector

Nothing to report.

[\[Return to top\]](#)

Emergency Services Sector

19. *September 18, Galveston County Daily News (TX)* — **LCVFD installs computer terminals in trucks.** The League City, TX, Fire Department (LCVFD) recently began installing mobile computer terminals in its fire trucks. **The computers will be capable of digitally mapping the most efficient route to fire calls, which will help cut response times.** Computer-aided dispatch from League City's center will automatically enter the address of fire calls into the fire truck computer, eliminating the need to type in the location. Taking street data directly from League City's Street Department will keep the department current on street closures, construction zones and new streets. Hydrant locations will be accurately plotted on the maps, so

crews will quickly learn the exact position of the closest water source. Access to satellite photography of the city will give firefighters the unprecedented ability to see hazards and obstructions that don't appear on paper maps, such as swimming pools and fences. **A database of chemicals and their properties will also be available, giving firefighters opportunities to diagnose situations involving hazardous materials from a safe distance.** Besides the mapping and routing capabilities, data modems will make wireless communication with dispatch possible, freeing up the voice radios for more urgent discussions.

Source: <http://www.galvnews.com/story.lasso?wcd=24073>

20. *September 18, Caller–Times (TX)* — **Hijacked bus, spill just part of the drill.** Emergency crews kept their cool under the blazing heat Friday, September 17, to neutralize a mock terrorist situation involving a hijacked school bus, a chemical spill and a bomb. **The San Patricio, TX, Local Emergency Planning Committee organized the drill, involving San Patricio, Aransas and Refugio counties to train for the unexpected.** Jane Ward, a committee member and chairwoman of the drill, said about 20 emergency departments participated in the exercise, which began at 8 a.m. with a simulated hijacking of a school bus filled with high school students heading west on State Highway 188. Another emergency task for hazardous material crews involved containing a chemical leak from a truck that supposedly was struck by the school bus. After the leak was secured, SWAT members charged the hijacked bus to arrest the driver, who was supposed to be a terrorist. Groups of students from Aransas Pass and Rockport high schools who volunteered to role–play as victims in the accident wore adhesive "wounds" and were treated by emergency officials.

Source: http://www.caller.com/ccct/local_news/article/0.1641.CCCT_81_1_3192195.00.html

[\[Return to top\]](#)

Information Technology and Telecommunications Sector

21. *September 17, Washington Post* — **Cash bounties for spammers win limited FTC backing.** The Federal Trade Commission (FTC), on Thursday, September 16, gave limited endorsement to offering cash rewards to people who help track down e–mail spammers, suggesting that such bounties might work but in fewer circumstances than had been pushed by some anti–spam activists. Congress asked the FTC to study two possible techniques as part of the first federal anti–spam law passed late last year. In June, the FTC recommended against the first technique, a do–not–spam registry, saying it would not work and might lead to more spam. The notion of bounties drew particular credence when it was pushed by Lawrence Lessig, a Stanford University law professor and one of the country's foremost thinkers on cyberspace law and policy. But the major Internet providers, who have their own spam–fighting operations, counseled the FTC against the idea. An America Online Inc. spokesperson, Nicholas J. Graham, said the use of bounty hunters can create its own set of legal problems that could complicate prosecutions. **The commission estimates that rewards would need to be in the range of \$100,000 to \$250,000, which Congress would need to fund because those amounts are unlikely to be covered by damages won in court.**

Source: http://www.washingtonpost.com/wp–dyn/articles/A27220–2004Sep_16.html

22. *September 17, US–CERT* — **Technical Cyber Security Alert TA04–261A: Multiple vulnerabilities in Mozilla products.** Several vulnerabilities exist in the Mozilla web browser

and derived products, the most serious of which could allow a remote attacker to execute arbitrary code on an affected system. Mozilla has released versions of the affected software that contain patches for these issues: Mozilla 1.7.3, Firefox Preview Release, Thunderbird 0.8.

Users are strongly encouraged to upgrade to one of these versions available at:

www.mozilla.org

Source: <http://www.uscert.gov/cas/techalerts/TA04-261A.html>

23. *September 16, iDEFENSE* — **Ipswitch WhatsUp Gold remote denial of service vulnerability.** Remote exploitation of a denial of service vulnerability in Ipswitch Inc.'s WhatsUp Gold version versions 8.03 and the latest version 8.03 Hotfix 1 allows attackers to cause the application to crash. Successful exploitation allows unauthenticated remote attackers to crash the WhatsUp Gold application. A patch is available at:

<http://www.ipswitch.com/Support/WhatsUp/patch-upgrades.html>

Source: <http://www.idefense.com/application/poi/display?id=142&type=vulnerabilities&flashstatus=true>

24. *September 16, InfoWorld* — **FBI seizes \$87 million worth of illegal software.** A two-year investigation by U.S. law enforcement authorities has resulted in one of the largest seizures of fake software ever in the U.S. and charges against 11 individuals. **The defendants from California, Washington, and Texas were indicted, Wednesday, September 15, with conspiring to distribute counterfeit computer software and documentation with a retail value of more than \$30 million, the U.S. Attorney's Office for the Central District of California said in a statement.** The value could rise to \$87 million, U.S. Attorney's Office spokesperson Thom Mrozek said. When arresting the defendants and searching their homes, offices and storage facilities, Federal Bureau of Investigation agents uncovered an additional stockpile of more than \$56 million worth of fake Microsoft Corp., Symantec Corp. and Adobe Systems Inc. products. Microsoft worked closely with the authorities in Los Angeles on the case, which was code-named "Digital Marauder."

Source: http://www.infoworld.com/article/04/09/16/HNfbi_1.html

25. *September 15, Westpoint Security Advisory* — **Several Internet browsers have session fixation vulnerability.** A vulnerability was reported in Microsoft Internet Explorer, KDE Konqueror, Mozilla Firefox, and Opera that may allow a remote user to set cookies on via a non-secure server to be sent to a secure server as part of a Session Fixation Attack. This flaw may allow remote users to hijack a target user's session. No solution is currently available; refer to Westpoint Security Advisory for workarounds.

Source: <http://www.westpoint.ltd.uk/advisories/wp-04-0001.txt>

Internet Alert Dashboard

DHS/US-CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US-CERT Operations Center Synopsis: Microsoft released a new security bulletin detailing critical vulnerabilities in the way it handles JPEG graphics. More information can be found here:
<http://www.microsoft.com/technet/security/bulletin/ms04-028.msp>.

Current Port Attacks

Top 10 Target Ports	445 (microsoft-ds), 135 (epmap), 1434 (ms-sql-m), 9898 (dabber), 5554 (sasser-ftp), 137 (netbios-ns), 1433 (ms-sql-s), 4899 (radmin), 1023 (Reserved), 21 (ftp) Source: http://isc.incidents.org/top10.html ; Internet Storm Center
----------------------------	--

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[[Return to top](#)]

Commercial Facilities/Real Estate, Monument & Icons Sector

26. *September 19, Plain Dealer (OH)* — Statue of Liberty worth visit despite new security.

Security is high at the nation's symbol of freedom and even more intense since the National Park Service reopened the statue's pedestal to the public last month. **Closed after the September 11 terrorist attacks, the pedestal and statue underwent \$7 million of restoration and security improvements, including the elaborate fencing.** Though Liberty Island was reopened to the public in December 2001 while crews worked, taking a traditional tour inside the statue was prohibited. **Now, the closest visitors can get to the lady are her feet; trips to her crown are a thing of the past.** Visitors are subjected to an intense search at Battery Park in New York City, similar to security at airports. All bags, purses and briefcases are put through an X-ray machine monitored by guards, who routinely ask that watches, bracelets and sometimes even shoes be removed and placed in a tray before allowing visitors to walk through metal detectors.

Source: <http://www.cleveland.com/living/plaindealer/index.ssf?/base/living/1095413833297491.xml>

[[Return to top](#)]

General Sector

Nothing to report.

[[Return to top](#)]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP Web page (<http://www.nipc.gov>), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Alerts – Advisories and Information Bulletins: DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Daily Open Source Infrastructure Reports – The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open-source published information concerning significant critical infrastructure issues.

DHS/IAIP Daily Reports Archive – Access past DHS/IAIP Daily Open Source Infrastructure Reports.

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions: Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883-3644.

Subscription and Distribution Information: Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883-3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.